



Zero Trust Access

Zero Trust by Deloitte offers a broad range of services to help organizations align to the ‘*never trust, always verify*’ cyber approach while securing the ubiquitous nature of their modern enterprises.

Zero Trust Access, a component of this broad portfolio, is a managed service that can accelerate this journey by securely connecting what matters: users to applications.

Organizations across industries are realizing that legacy and perimeter-based approaches are no longer suitable to protect the enterprise and spearhead business enablement. This is due to the likelihood that their data no longer resides within the fortified walls of their data centers. Accelerated adoption of cloud computing and digital transformation, shifting workforce dynamics, and the need to secure increasingly hyper-connected information technology (IT) ecosystems have led to a new paradigm.

Zero Trust is a conceptual framework that commits to removing implicit trust within the IT ecosystem, replacing it with a risk-based approach that continuously verifies each connection and implements granular access control to enterprise resources.

Deloitte's Zero Trust Access (ZTA) is designed to help address the evolving requirements of enterprises so they can confidently protect their applications, infrastructure, and data. Through this solution, Deloitte offers a cloud-native managed service that secures communications between end user devices, and enterprise applications, wherever they may reside.

Grounded upon Zero Trust principles, Zero Trust Access assists enterprises to adopt a “least-privilege” policy for applications and users across Software-as-a-Service (SaaS) and private applications in public or private cloud environments. The capability can replace legacy remote access technology with a modern Deloitte managed service or complement a broader ecosystem of technologies and capabilities to accelerate Zero Trust adoption. The service can also significantly reduce the





total cost of ownership (TCO) associated with legacy technologies and the burden on operational teams to maintain them.

With innovative microcontainer-based data protection, Deloitte's Zero Trust Access helps organizations to protect sensitive information, prevent data exfiltration, and potentially replace costly and complex legacy solutions.

The service provides a turnkey solution that accelerates Zero Trust connectivity with application segmentation and inherent data protection capabilities – relieving IT and security teams of the cost and complexity associated with building and maintaining their own infrastructure to achieve similar outcomes.





Common use cases

While Deloitte's Zero Trust Access is applicable to a variety of scenarios, below are some prevalent use cases driving adoption in the marketplace.

 Secure Remote Access	 Mergers & Acquisitions	 Third Party Access	 Attack Surface Management
Replace legacy remote access solutions such as virtual private network (VPN) or virtual desktop infrastructure (VDI) with a cloud-native service that is inherently scalable, resilient, and secure.	Prevent exfiltration of sensitive data during the mergers and acquisition (M&A) lifecycle; provision and secure access to enterprise applications without the complexity of integrating IT ecosystems.	Provision least privilege access and data protection for third-party access to enterprise resources. Control access to applications that require heightened security (e.g., copy/paste or download prevention) and apply granular access controls based on the sensitivity and regulatory requirements of the underlying data.	Reduce Internet-facing footprint and exposure by hiding sensitive resources and requiring pre-authentication and continuous authorization to establish and maintain user connectivity.

Benefits

Benefits of Deloitte's Zero Trust Access solution may be realized through its implementation across a myriad of use cases.

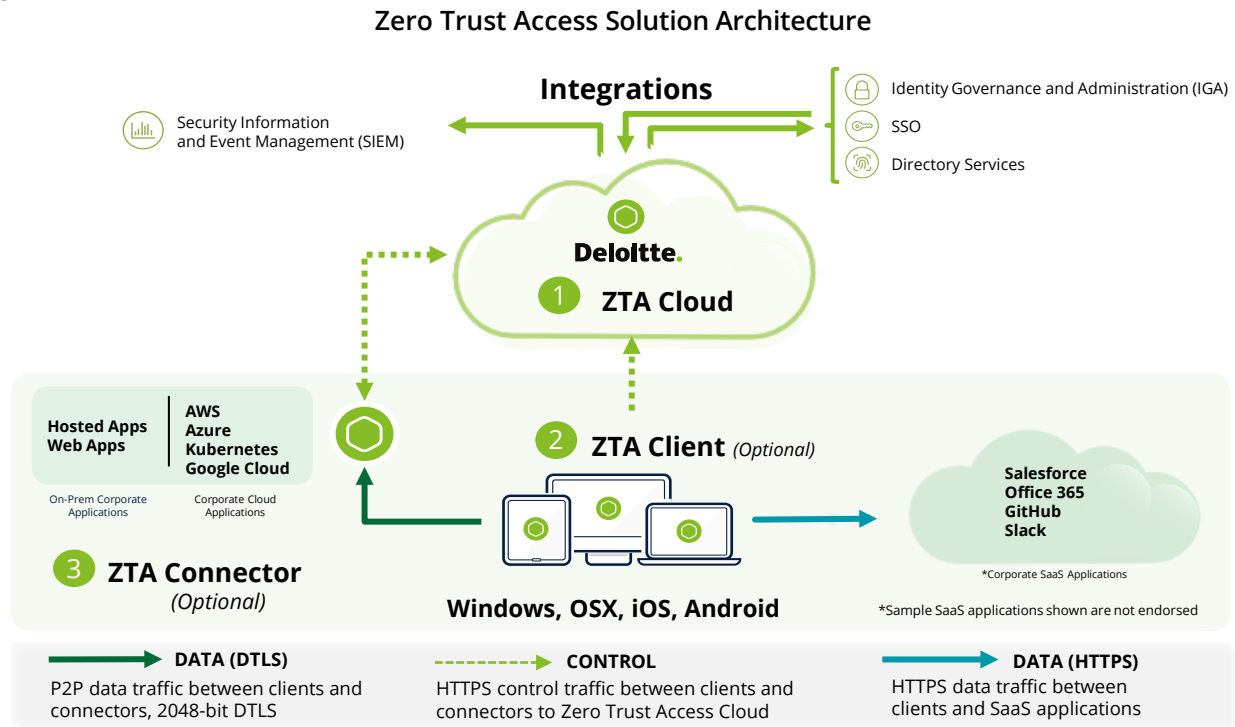
 Enhanced Security, Less Complexity	 Enhanced User Productivity	 Cost Reduction, Ease of Operations	 Business Agility
With Deloitte's Zero Trust Access, resources can be hidden from the internet and accessed only after authentication and authorization, while built-in application segmentation mitigates lateral movement threats. The cloud-delivered service requires minimal changes to underlying network topology and security configuration, simplifying adoption and use.	Deloitte's Zero Trust Access provides an efficient user experience with minimal impact on the end user experience. Browser-based workflow makes it easy to onboard users and the service retains an 'on-device' experience which can enhance workforce productivity.	Deloitte's Zero Trust Access does not require the capital expenditure that's typically associated with infrastructure investments or other depreciating assets. Cost is based on a simple, scalable, efficient, and predictable operational expense (OPEX) model. Deloitte operates Zero Trust Access as a managed service which also relieves the operational burden on IT and security teams.	Deloitte's Zero Trust Access facilitates anytime, anywhere application access for various types of applications (e.g., legacy hosted applications, thick-client applications, web-based applications, SaaS) from managed or unmanaged devices, providing the flexibility for IT to keep pace with changing business demands.

Why Deloitte?

 We have a broad portfolio of Zero Trust advisory, implementation, and managed services. Our breadth and depth as well as leading ecosystem and alliance relationships allows us to provide the outcomes (and value) you seek as a trusted advisor, a technology-savvy pioneer, a visionary integrator, and a dependable operating guide.

Zero Trust Access

Deloitte's Zero Trust Access comprises three essential components that collectively provide secure and ephemeral access to enterprise resources, wherever they may reside. These components, the interaction between them, and the functionality that each serves are expressed in the diagram below:



1 ZTA Cloud

- Brokers a secure and ephemeral connection between a user and target application
- Integrates with identity and access management (IAM) technologies
- Enables policy configuration

2 ZTA Connector





- Deployed in data centers or cloud environments near target applications
- Initiates outbound connection to the ZTA Cloud
- Common server operating system (OS) compatibility

3 ZTA Client

- Runs as a lightweight application on end user devices without administrator privileges, which is desirable for unmanaged devices
- Common mobile and endpoint OS compatibility
- Enforces data protection for data at rest and in transit

Zero Trust Access Features

Deloitte's Zero Trust Access solution architecture enables advanced security features, including, but not limited to, the following:

 Zero Trust Network Access (ZTNA)	 Continuous Authorization	 Ephemeral Connectivity	 Built-in Data Protection
Software defined perimeter (SDP) architecture, coupled to application segmentation capabilities, removes the need to provision inbound network access to sensitive resources. Connecting users directly to target applications vs. broad network access prevents lateral movement risks by making the underlying networks inaccessible to the user.	Authorization is re-examined in periodic intervals after initial access and can be dynamically adjusted based on contextual security information such as device security posture, location, time of day, and device integrity.	The cloud component brokers each connection and tears it down upon session completion. Peer-to-peer (P2P) communication between the end user and target application allows for data traffic to flow directly between the source and destination, rather than traversing third party environments - virtually eliminating man-in-the-middle threats.	Data at-rest, in-use, and in-transit is secured through strong encryption, configurable control over print/copy/paste features, anti-keylogging, anti-screen scraping, watermarking, remote data destruction, and other built-in data protection features.

Contact us



Deborah Golden
Principal
Cyber & Strategic Risk Leader
Deloitte & Touche LLP
Office: +1 571 882 5106
debgolden@deloitte.com



Andrew Rafla
Principal
Zero Trust Offering Leader
Deloitte & Touche LLP
Office: +1 201 499 0580
arafla@deloitte.com



Egemen Tas
Managing Director
Zero Trust Product Leader
Deloitte & Touche LLP
Office: +1 201 499 0547
egtas@deloitte.com



Chalan Aras
Managing Director
Products & Services Leader
Deloitte & Touche LLP
Office: +1 408 704 4897
chaaras@deloitte.com

This document contains general information only and Deloitte is not, by means of this document, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This document is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this document.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2023 Deloitte Development LLC. All rights reserved.